JENAYAH ALAM MAYA

ALAM MAYA

HASNIZA HUSSAIN

Bukan baru isu jenayah siber diperkatakan. Walaupun pendedahan demi pendedahan dibuat, kesedaran masyarakat di negara ini masih di tahap mengecewakan.

Persoalannya, mengapa masyarakat seolah-olah tidak menyedari kewujudan jenayah Internet ini? Adakah informasi masih tidak cukup?Atau sikap tidak endah menjadi punca kenapa mereka sengaja membutakan mata dan memekakkan telinga untuk menerima maklumat yang mungkin tidak seratus peratus melindungi mereka.

Terdapat kemungkinan masyarakat tidak kisah kerana hal penipuan alam maya belum terjadi kepada mereka. Walau apa pun sikap masyarakat kita pada hari ini, peranan penulis untuk menyampaikan maklumat secara berterusan tetap dilakukan tanpa jemu. Apa yang penting, masyarakat perlu ubah sikap untuk mengetahui apa yang terjadi di sekeliling mereka.

Kategori jenayah

1) Parcel
2) Penyamaran
3) Khidmat pesanan ringkas (SMS)/panggilan
4) Pembelian/penipuan Internet
5) Perbankan Internet (Phishing)

Modus operandi

1 Parcel

Suspek akan cari mangsa melalui laman sosial di Internet antaranya Friendster, Facebook, Tagged, Myspace.

- Supek akan berpura-pura berkenalan dan menjalin hubungan cinta dengan mangsa
- Mangsa kemudiannya dijanjikan dengan penghantaran barangan berharga seperti wang tunai, barang kemas dan lain-lain.
- Suspek akan minta mangsa buat pembayaran untuk caj penghantaran, cukai kastam dan pertukaran mata wang asing menerusi akaun bank yang diberi.
- Mangsa hanya sedar ditipu apabila bungkusan dijanjikan tidak diterima dan suspek menghilangkan diri.

2 Penyamaran

Suspek atau sindiket menyamar sebagai kakitangan institusi kewangan guna teknik 'spoofing' iaitu dengan menghubungi mangsa melalui telefon.

- Suspek akan maklumkan bahawa mangsa mempunyai hutang kad kredit atau terlibat dalam aktiviti haram.
- Teknik spoofing adalah teknik di mana pemanggil akan guna perisian tertentu bagi membolehkannya meletakkan sebarang nombor untuk memperdaya mangsa mempercayai pemanggil adalah dari nombor yang tertera di skrin.
- Mangsa diminta hubungi seseorang yang kononnya pegawai dari Bank Negara yang boleh membantu untuk selesaikan perkara terbabit.
- Mangsa yang terpedaya akan diarahkan untuk memindahkan wang dari akaunnya ke akaun yang diberikan suspek.
- Mangsa sedar diri tertipu apabila wang dalam akaun berkurangan/lesap.

3 SMS/panggilan

Sindiket akan perdaya mangsa melalui SMS yang menyatakan mangsa memenangi hadiah peraduan. Contoh: Power Root, Shell, Celcom

- Mangsa kemudiannya diminta mendepositkan sejumlah wang sebagai syarat untuk memperolehi hadiah.
- Biasanya mangsa akan ke bank dan mendepositkan wang seperti diarahkan suspek/sindiket ke dalam akaun diberikan.
- Mangsa sedar ditipu apabila tidak menerima hadiah dijanjikan.

4 Pembelian/penipuan Internet

- Suspek iklankan penjualan barangan di Internet dan minta mangsa buat pembayaran untuk beli barangan.
- Setelah pembayaran dibuat, barangan dibeli tidak diterima dan suspek menghilangkan diri.

5 Perbankan Internet (phishing)

- Penjenayah guna teknik phishing dengan wujudkan satu laman web sama seperti laman web sebenar sesebuah bank dan umpan pengguna melalui emel agar pengguna dedahkan maklumat perbankan Internet tanpa disedari.
- Penjenayah akan hantar emel berbentuk 'security alert' yang mengarahkan mangsa supaya kemaskini akaun mereka bagi tujuan keselamatan bank
- Mangsa diminta memasukkan username, password dan nombor TAC dalam proses kemaskini itu.
- Mangsa hanya mengetahui ditipu apabila menerima SMS daripada pihak bank yang menyatakan wang telah dipindahkan ke akaun pihak ketiga

Nasihat kepada orang ramai

- Jangan terpengaruh dengan tipu helah (modus operandi) suspek.
- Waspada dengan pemberian hadiah (benda berharga), SMS dan telefon yang akan diberikan oleh orang yang tidak dikenali.
- Bertindak bijak jika dihampiri atau cuba diperdaya sindiket/suspek. Mengecam suspek sebaik mungkin dan segera bertindak.
- Selidik untuk pastikan kesahihan agensi syarikat atau orang perseorangan yang menawarkan untuk beri bungkusan hadiah bagi mengelak ditipu.
- Sentiasa berhati-hati dengan individu yang dikenali melalui Internet terutamanya yang menjanjikan tawaran hadiah dari luar negara.
- Jangan sesekali memasukkan wang ke dalam akaun individu yang tidak dikenali sekiranya arahan terbabit melalui telefon, SMS dan emel.
- Dapatkan pengesahan daripada Jabatan Siasatan Jenayah Komersil (JSJK), Polis Diraja Malaysia (PDRM) (03-26163999/03-26163822).

Statistik kes/ tangkapan

JENIS: Parcel
2010 - jumlah kes: 791
Kerugian: RM18, 992, 366.27
Tangkapan: -
JAN-MAC 2011: Jumlah kes: 245
Kerugian: RM 376, 5683. 93
Tangkapan : -

JENIS: Penyamaran
2010 - Jumlah kes: 1201
Kerugian: RM20, 786, 906. 62
Tangkapan: 3 orang
JAN-MAC 2011: Jumlah kes: 104
Kerugian: RM7, 687, 370. 09
Tangkapan: -

JENIS: SMS/Panggilan
2010 - Jumlah kes: 836
Kerugian: RM9, 695, 112.50
Tangkapan: -
JAN-MAC 2011: Jumlah kes: 137
Kerugian: RM 348, 276.55
Tangkapan: -

JENIS: Pembelian/penipuan Internet
2010 - Jumlah kes: 1, 114
Kerugian: RM3,124, 836.72
Tangkapan: -
JAN-MAC 2011: Jumlah kes: 459
Kerugian: RM801, 802.15
Tangkapan: -

JENIS: Perbankan Internet (phishing)
2010 - jumlah kes: 353
Kerugian: RM 1, 244, 363.45
Tangkapan: -
JAN-Mac 2011: Jumlah kes: 306
Kerugian: RM 991, 474. 07
Tangkapan: -

Sumber: JSJK, PDRM